PATENT
1110-0297P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	Naoto KINJO	Conf.:	6316
Appl. No.:	09/981,920	Group:	
Filed:	October 19, 2001	Examiner:	

METHOD OF PREVENTING FALSIFICATION OF IMAGE

L E T T E R

Assistant Commissioner for Patents
Washington, DC 20231

January 9, 2002

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
JAPAN	2000-320229	October 20, 2000

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____
Michael K. Mutter, #29,680

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

MKM/lab
1110-0297P

Attachment

(Rev. 10/31/01)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１０月２０日

出願番号
Application Number: 特願２０００－３２０２２９

出願人
Applicant(s): 富士写真フイルム株式会社

２００１年 ９月１０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３０８３１３５

【書類名】　特許願
【整理番号】　FF887740
【提出日】　平成12年10月20日
【あて先】　特許庁長官　殿
【国際特許分類】　H04N 1/387
【発明の名称】　撮影画像の改竄防止方法
【請求項の数】　2
【発明者】
【住所又は居所】　神奈川県足柄上郡開成町宮台７９８番地　富士写真フイルム株式会社内
【氏名】　金城　直人
【特許出願人】
【識別番号】　000005201
【氏名又は名称】　富士写真フイルム株式会社
【代理人】
【識別番号】　100080159
【弁理士】
【氏名又は名称】　渡辺　望稔
【電話番号】　3864-4498
【手数料の表示】
【予納台帳番号】　006910
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9800463
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　撮影画像の改竄防止方法

【特許請求の範囲】

【請求項１】

カメラにおいて、撮影画像から特定アルゴリズムにより画像特徴量を抽出し、

カメラの撮影画像識別情報と前記画像特徴量を、撮影画像に改竄がないことを認証する認証機関のデータベースに記録し、

前記認証機関において、認証することを請求された認証対象画像について、該認証対象画像から前記特定アルゴリズムにより画像特徴量を抽出し、該抽出された画像特徴量を前記データベースに記録された画像特徴量と比較し、

該比較における両画像特徴量の一致度により、前記認証対象画像に撮影後の改竄がないことを判定することにより、撮影画像の改竄を防止することを特徴とする撮影画像の改竄防止方法。

【請求項２】

撮影画像に改竄がないことを認証する認証機関からカメラに、前記認証のための認証用データを送付するとともに、前記認証用データと前記カメラの撮影画像識別情報を前記認証機関のデータベースに記録し、

前記カメラは画像撮影の際、該撮影画像に前記認証用データを付属させるか、または埋め込むようにし、

前記認証機関において、認証することを請求された認証対象画像について、該認証対象画像から前記認証用データを抽出し、該抽出した認証用データを前記データベースに記録された認証用データと比較し、

該比較における両認証用データの一致度により、前記認証対象画像に撮影後の改竄がないことを判定することにより、撮影画像の改竄を防止することを特徴とする撮影画像の改竄防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルスチルカメラ等で撮影されたデジタル画像データに改竄が

ないことを認証することでデジタル画像データの改竄を防止する撮影画像の改竄防止方法に関する。

【０００２】

【従来の技術】

従来、銀塩写真技術における露光系では、一般にアナログ露光（面露光、直接露光）によってプリントが行われていた。すなわち、現像済みのネガフィルムを所定の焼き付け位置に位置決めして、白色光源（ハロゲンランプ等）からの光を照射し、ネガフィルムからの透過画像を印画紙に結像して露光していた。

【０００３】

これに対して、近年では、デジタル露光を利用する焼き付け装置、すなわち、ネガフィルムやカラーリバーサルフィルム等の写真フィルムに記録された画像を光電的に読み取って、読み取った画像をデジタル信号とした後、種々のデジタル画像処理を施して記録用の画像データとし、この画像データに応じて変調した記録光によって感光材料を走査露光して画像（潜像）を記録し、（仕上がり）プリントとするデジタルフォトプリンタが実用化されている。

【０００４】

このようなデジタルフォトプリンタにおいては、画像をデジタル画像データとして取り扱うので、写真フィルムに撮影された画像のみならず、デジタルスチルカメラ（ＤＳＣ）等で撮影された画像や、ＣＤ－Ｒやフロッピーディスク、リムーバブルハードディスク（Ｚｉｐ、Ｊａｚ等）等の磁気記録媒体、ＭＯディスク（光磁気記録媒体）等の各種の記録媒体にデジタルデータとして記録された画像データについても、画像処理を施してプリントとして出力することができる。

【０００５】

このようなデジタルデータは、パソコン等の情報処理、情報通信機器とのデータの接続、転送が容易である反面、データの取り扱いの容易さから、比較的自由にデータの改竄がなされ易いという欠点があり、データの改竄の防止や、データの正当性の認証が困難であった。

例えば、従来自動車保険等の損害クレーム処理において、損害の査定に用いられる証拠写真としてデジタルカメラによって撮影された写真画像を用いた場合に

、その写真画像の改竄や、すり替え（写真の偽造）による不正をいかにして見破り、また防止するかということが問題となっていた。

【０００６】

これに対する一つの提案が電子情報通信学会技術研究報告になされている。「保険クレーム処理グループワークシステムにおけるデジタル写真の改ざん防止と検出機能」（豊川和治、森本典繁、利根川聡子、上條浩一、小出昭夫、信学技報、１９９９年９月、ｐ．１～ｐ．８、ＩＥ９９－３８）である。これは、査定員が、特別のＩＤや認証キーを書き込んだメモリカードを装着したデジタルカメラで事故車両の撮影を行うと、デジタルカメラにより自動的に、撮影日時と認証マークがメモリカードに書き込まれ、このメモリカードを、コンピュータのメモリカード読み取り用デバイスドライバで読み取ると、認証マークの存在により、撮影写真が修正されたものではなく真正のものであることが保証されるというものである。

【０００７】

また、従来メモリカード等の記録媒体による画像データの受け渡しの他、通信回線を通じて画像データを転送することも行われている。この場合、データ転送中に、第三者によってデータが不正に改竄されたり、すり替えられたりする虞があるため、通信におけるセキュリティ保護が問題となっている。

これに対して、従来例えば、そのデータの正当性を保証する情報を暗号化して送る方法や、電子署名等の方法、あるいは画像中に視認不可能な情報を埋め込む電子透かしの技法等により、データのすり替えや、改竄の防止を図る様々な方法が考えられている。

【０００８】

【発明が解決しようとする課題】

しかしながら、前記公報に開示されたものでは、特定のプロトコルを用いてカメラからメモリカードを経由してデータの授受を行っているため、特別なハードウェア認証機能を持たせたメモリカードを必要としており、不特定多数のユーザを対象とする場合には不向きであるという問題がある。従って、このように特殊な機能を持たせた記録媒体を必要とせずに、画像の改竄がないことを認証するシ

ステムの実現が望まれていた。

また、前述したように、データの暗号化や電子透かしの方法等による通信データのセキュリティ保護の様々な方法が開発されてはいるが、真に効果的な、画像データの改竄防止方法というものは、まだ存在しない。

【０００９】

本発明は、前記従来の問題に鑑みてなされたものであり、特殊な機能を持たせた記録媒体を必要とせずに、画像の改竄がないことを認証することにより、画像の改竄を効果的に防止することのできる撮影画像の改竄防止方法を提供することを課題とする。

【００１０】

【課題を解決するための手段】

前記課題を解決するために、本発明の第一の態様は、カメラにおいて、撮影画像から特定アルゴリズムにより画像特徴量を抽出し、カメラの撮影画像識別情報と前記画像特徴量を、撮影画像に改竄がないことを認証する認証機関のデータベースに記録し、前記認証機関において、認証することを請求された認証対象画像について、該認証対象画像から前記特定アルゴリズムにより画像特徴量を抽出し、該抽出された画像特徴量を前記データベースに記録された画像特徴量と比較し、該比較における両画像特徴量の一致度により、前記認証対象画像に撮影後の改竄がないことを判定することにより、撮影画像の改竄を防止することを特徴とする撮影画像の改竄防止方法を提供する。

【００１１】

また、同様に前記課題を解決するために、本発明の第二の態様は、撮影画像に改竄がないことを認証する認証機関からカメラに、前記認証のための認証用データを送付するとともに、前記認証用データと前記カメラの撮影画像識別情報を前記認証機関のデータベースに記録し、前記カメラは画像撮影の際、該撮影画像に前記認証用データを付属させるか、または埋め込むようにし、前記認証機関において、認証することを請求された認証対象画像について、該認証対象画像から前記認証用データを抽出し、該抽出した認証用データを前記データベースに記録された認証用データと比較し、該比較における両認証用データの一致度により、前

記認証対象画像に撮影後の改竄がないことを判定することにより、撮影画像の改竄を防止することを特徴とする撮影画像の改竄防止方法を提供する。

【００１２】

【発明の実施の形態】

以下、本発明に係る撮影画像の改竄防止方法について、添付の図面に示される好適実施形態を基に、詳細に説明する。

【００１３】

まず本発明の第一実施形態について説明する。本実施形態は、カメラにおいて撮影画像から抽出した所定の画像特徴量データを認証機関に送っておき、認証機関はこの画像特徴量データを用いて画像の認証を行うようにするものである。

図１は、本発明の第一実施形態に係る撮影画像の改竄防止方法を実施するシステムの概略を示すブロック図である。

【００１４】

図１において、認証機関１０は、ある撮影画像が、該認証機関１０に登録された正しいカメラ２０により撮影され、撮影後改竄されていない真正の画像であることを認証するものである。カメラ（デジタルスチルカメラ）２０は、予め認証機関１０に登録されており、被写体３０を撮影する際には、認証機関１０と通信を行い、撮影画像の認証に必要な情報を認証機関１０に送るとともに、認証機関１０から登録の確認を受け、撮影画像をスマートメディア等の記録媒体４０に記録する。

また、認証機関１０は、カメラ２０から送られる撮影画像識別情報および画像特徴量等の撮影画像の認証に必要な情報を記録するデータベース１２を有している。

【００１５】

本実施形態におけるカメラによる撮影の方法を図２のフローチャートに、また画像の認証方法を図３のフローチャートに示す。以下、本実施形態の作用を、これらのフローチャートに沿って説明する。

なお、本実施形態においては、第三者が、認証機関１０に登録されている正規のカメラ２０に成り済まして偽造画像を伝送するのを防ぐために、データの送受

信はすべて暗号化して行うものとする。

【００１６】

まず図２のフローチャートに沿って、カメラによる撮影の方法について説明する。ステップ１００において、予めカメラ２０を認証機関１０に登録しておく。事前にカメラ２０には、カメラ出荷時あるいは発売時において、カメラ固有のＩＤと暗号用鍵データが割りつけられている。これらのカメラ固有のＩＤ情報を認証機関１０に登録しておく。したがって、このカメラの登録は、はじめに一回だけやっておけばよい。

【００１７】

以下、カメラ２０で撮影する場合には、まずステップ１１０において、これから撮影するカメラが認証機関１０に登録したものであることを、認証機関１０に確認（認証）してもらう。そのためカメラ２０は、データ登録依頼信号（カメラが登録されたものであることを確認するために必要な情報）を認証機関１０に送信する。すなわち、カメラ２０は、カメラＩＤ情報等を暗号化して認証機関１０に送信する。認証機関１０は、カメラ２０から暗号化されたデータ登録依頼信号を受け取ると、これを解読し、カメラ２０が登録済であることを確認する。

この暗号を用いてカメラ２０が登録されたものであることを確認する方法は、特に限定されるものではなく、公知の暗号技術を用いることができる。例えば、Interface 誌、２０００年２月号、ｐ．148 ～ｐ．149 に暗号を用いた認証方法の一例が開示されている。

【００１８】

認証機関１０によってカメラ２０がすでに認証機関１０に登録されたものであることが確認されたら、次にステップ１２０において、カメラ２０は被写体３０を撮影する。

撮影後、ステップ１３０において、カメラ２０は、後に認証機関１０が画像の正当性を認証する際に用いるための画像特徴量データを、撮影された画像データから、特定のアルゴリズムにより作成する。

【００１９】

また、前記画像特徴量データを作成する特定のアルゴリズムとしては、特に限

定されるものではなく、例えば、画像を所定サイズのエリア（ブロック）に分割した後、各ブロック毎のエッジや空間周波数あるいはヒストグラムを計算する等が考えられる。このアルゴリズムは、例えば、特徴量データ作成部としてハード化し、撮影素子と１チップ化してカメラ２０に組み込むことによって、通信途中での偽造画像の割り込みを防止することができる。

また、このアルゴリズムは非公開とすることが望ましい。さらに、万一解読されることを想定して、該アルゴリズムを複数種類準備しておき、撮影時にその都度カメラ２０側でランダムに選択するようにしてもよいし、認証機関１０からの指示信号によって選択するようにしてもよい。

【００２０】

このとき、カメラ２０側でアルゴリズムを選択した場合には、どのアルゴリズムを選択したかを示す選択情報を画像特徴量データに付加して認証機関１０に送るようにする。また、認証機関１０からの指示信号でアルゴリズムを選択した場合には、認証機関１０が指示信号をカメラ２０に送信してから所定時間経過後はカメラ２０からの信号を受け付けないようにすることで、カメラ２０を使用している者に悪意がある場合に、事前に作成された偽造画像の割り込み伝送を防止することができる。

【００２１】

次にステップ１４０において、カメラ２０は、いま作成した画像特徴量データと、撮影画像識別情報とを、それぞれ暗号化してセットで認証機関１０に送信する。ここで、撮影画像識別情報とは、例えば、ファイル名、カメラＩＤ等である。カメラ認証後、データの送受信は共通鍵（秘密鍵）方式で行う。これは共通鍵方式のほうがより演算量が小さいからである。例えば、最初に公開鍵方式で各カメラ固有の秘密鍵データを伝送し、これを画像特徴量データの暗号化に用いるようにする。あるいは、その他の周知の暗号方式を用いる。

また、上にも述べたように、カメラ側で画像特徴量データ作成アルゴリズムを選択した場合には、アルゴリズム選択情報が、画像特徴量データに付加されて送られる。

認証機関１０は、これらの受け取った画像特徴量データや撮影画像識別情報を

データベース１２に記録する。このとき、採用された画像特徴量データ作成アルゴリズムの種類も合わせて記録する。

【００２２】

ステップ１５０において、認証機関１０が、上記受信信号を解読し、認証済みカメラのデータであることを確認した場合には、受け取り確認信号をカメラ２０へ返送する。

次にステップ１６０において、カメラ２０がこの確認信号を受け取ると、カメラ２０は、撮影画像を記録媒体４０に記録する。このとき、撮影画像には、前記撮影画像識別情報をヘッダとして付属させる。

【００２３】

カメラ２０による撮影処理は、以上のようにして行われる。このようにして撮影された画像を記録した記録媒体４０を受け取った者は、記録されている画像データを画像識別情報とともに、所定の通信手段により認証機関１０に送信して、その画像の正当性の認証を依頼する。

以下、認証処理について、図３のフローチャートを用いて説明する。

【００２４】

撮影画像を受け取った者が、画像の改竄チェックを認証機関１０へ依頼する場合、まずステップ２００において、画像データを認証機関１０に伝送する。

次にステップ２１０において、画像データを受け取った認証機関１０は、画像データのヘッダに付属された撮影画像識別情報を用いて、データベース１２より以前記録したこの画像に対応する画像特徴量データを読み出す。

【００２５】

また、ステップ２２０において認証機関１０は、前にカメラ２０で撮影時に採用された画像特徴量データ作成アルゴリズムと同じアルゴリズムによって、チェック対象画像（認証対象画像）から画像特徴量データを作成する。前述したように、この撮影時に採用されたアルゴリズムの種類も、データベース１２に記録されているため、データベース１２からこの種類を読み出して同じアルゴリズムを使用することができる。

【００２６】

次にステップ２３０において、チェック対象画像から作成した画像特徴量データと、データベース１２から読み出した画像特徴量データを比較する。

そして、両者の一致度を計算し、一致度が所定値以上の場合には、ステップ２４０において、チェック対象画像は撮影後の改竄はないものと判定する。ここで、両者の一致度が完全に一致することまでは要求せず、一致度が所定値以上でよいとしたのは、カメラ記録時におけるＪＰＥＧ等の圧縮処理により情報の劣化が起こっている可能性があるため、元画像と完全に一致するとは限らないためである。

【００２７】

このように、本実施形態によれば、偽造画像を認証済カメラによって撮影された画像であると偽装するケースに有効に対処することができ、撮影画像の改竄を効果的に防止することができる。

【００２８】

次に、本発明の第二実施形態について説明する。

第二実施形態は、カメラ側で撮影画像データに識別情報を埋め込んでおき、認証機関側では、これを用いて画像の認証を行うようにするものである。

【００２９】

図４に、本実施形態の方法を実施するシステムの概略を示す。

図４において、認証機関５０は、ある撮影画像が、該認証機関５０に登録された正しいカメラ６０により撮影され、撮影後改竄されていない真正の画像であることを認証するものである。カメラ（デジタルスチルカメラ）６０は、予め認証機関５０に登録されており、被写体７０を撮影する際には、認証機関５０と通信を行い、認証機関５０から送られた透かし情報（認証用データ）を撮影画像に埋め込み、透かし情報の埋め込まれた撮影画像をスマートメディア等の記録媒体８０に記録する。

また、認証機関５０は、カメラ６０から送られる撮影画像識別情報および画像特徴量等の撮影画像の認証に必要な情報を記録するデータベース５２を有している。

【００３０】

本実施形態におけるカメラによる撮影の方法を図５のフローチャートに、また画像の認証方法を図６のフローチャートに示す。以下、本実施形態の作用を、これらのフローチャートに沿って説明する。

【００３１】

まず図５のフローチャートに沿って、カメラによる撮影の方法について説明する。ステップ３００において、予めカメラ６０を認証機関５０に登録しておく。これは、第一実施形態と同様である。

次に、カメラ６０で撮影する場合には、ステップ３１０において、これから撮影するカメラが認証機関５０に登録したものであることを、認証機関５０に確認（認証）してもらう。そのためカメラ６０は、カメラＩＤ等を含むデータ登録依頼信号を認証機関５０に送信する。認証機関５０は、カメラ６０から暗号化されたデータ登録依頼信号を受け取ると、これを解読し、カメラ６０が登録済であることを確認する。

【００３２】

次に、ステップ３２０において、認証機関５０は、撮影画像ファイルに固有の透かし情報（認証用データ）を生成し、カメラ６０へ返送する。また、認証機関５０は、カメラＩＤ、画像ファイル名、受け付け日時、時刻等とともに前記透かし情報をデータベース５２に記録する。

ステップ３３０で、カメラ６０は被写体７０を撮影する。そして、ステップ３４０において、カメラ６０は、認証機関５０から返送された透かし情報を解読し、撮影画像に透かし情報の埋め込みを行う。

【００３３】

この埋め込み方法は、特に限定されるものではなく、公知の埋め込みアルゴリズムを用いることができる。しかし、どのような埋め込みアルゴリズムを用いたかは、非公開としたほうがよい。あるいは、埋め込みアルゴリズムを複数種類用意しておき、カメラ６０側でランダムに選択するようにしてもよいし、認証機関５０からの返送情報に含まれる選択信号によって切り換えるようにしてもよい。この場合、認証機関５０では、どのアルゴリズムが採用されたかという情報もデータベース５２に記録しておく。また、カメラ６０側で、撮影画像データのヘッ

ダ情報として、透かし情報の識別データを付加するようにしてもよい。

【００３４】

次に、ステップ３５０において、カメラ６０は、透かし情報の埋め込まれた撮影画像データを記録媒体８０に記録する。

カメラ６０による撮影処理は、以上のようにして行われる。このようにして撮影された画像を記録した記録媒体８０を受け取った者は、記録されている画像データを所定の通信手段により認証機関５０に送信して、その画像の正当性について認証を依頼する。

以下、認証処理について、図６のフローチャートに沿って説明する。

【００３５】

撮影画像を受け取った者が、画像の改竄チェックを認証機関５０に依頼する場合、まずステップ４００で、画像データを認証機関５０に伝送する。

次に、ステップ４１０において、画像データを受け取った認証機関５０は、画像データの画像ファイル名、ヘッダの透かし情報識別データにより、データベース５２から、データベースに記録されたチェック対象画像に対応する画像データの透かし情報を読み出す。

【００３６】

また、認証機関５０は、ステップ４２０において、チェック対象画像から透かし情報を抽出し、ステップ４３０において、チェック対象画像から抽出した透かし情報とデータベース５２から読み出した透かし情報とを比較する。比較の結果、一致度が所定値以上の場合には、ステップ４４０において、認証機関５０は、チェック画像には、改竄はないものと判定する。

【００３７】

このように、本実施形態によれば、画像データに透かし情報を埋め込むようにしたため、透かし情報を改変することなく、画像データのみを変えることは不可能であり、撮影画像を加工することにより画像を偽造するケースに対処することができ、撮影画像の改竄を効果的に防止することができる。

【００３８】

また、その他の例として、例えば、カメラによる撮影時に、カメラの多点測距

データを画像データ特徴量とセットで認証機関に伝送し、データベースに記録しておき、このデータを用いて認証処理を行う方法もある。これによれば、例えば、偽造画像プリントを撮影した偽造画像データの場合、その測距データから、被写体が平面であることがわかる。画像シーンが立体物である場合は、矛盾するので、認証時にこのような測距データと画像の矛盾点から改竄の判定をすることができる。

【００３９】

以上詳細に説明したように、本発明の各実施形態によれば、偽造画像を認証済カメラによる撮影画像と偽ったり、撮影画像を加工して認証機関を欺こうとする等のケースに対して、画像の改竄、偽造をチェックすることができる。

また、画像そのものでなく、画像特徴量等のみを登録するようにすることで、認証機関のデータ容量を低減し、効率的に画像改竄の判定および改竄防止を図ることができる。

【００４０】

以上、本発明の撮影画像の改竄防止方法について詳細に説明したが、本発明は、以上の例には限定されず、本発明の要旨を逸脱しない範囲において、各種の改良や変更を行ってもよいのはもちろんである。

【００４１】

【発明の効果】

以上説明した通り、本発明によれば、偽造画像を認証済カメラによる撮影画像であると偽ったり、撮影画像を加工して認証機関を欺こうとする等のケースに対して、特殊な機能を持たせた記録媒体等を必要とせずに、撮影画像の改竄の有無を判定し、効果的に画像の改竄を防止することができる。

【図面の簡単な説明】

【図１】　本発明の第一実施形態に係る撮影画像の改竄防止方法を実施するシステムの概略を示すブロック図である。

【図２】　第一実施形態におけるカメラによる撮影の方法を示すフローチャートである。

【図３】　同じく、第一実施形態における認証処理方法を示すフローチャート

である。

【図４】　本発明の第二実施形態の方法を実施するシステムの概略を示すブロック図である。

【図５】　第二実施形態におけるカメラによる撮影の方法を示すフローチャートである。

【図６】　同じく、第二実施形態における認証処理方法を示すフローチャートである。

【符号の説明】

１０、５０　認証機関

１２、５２　データベース

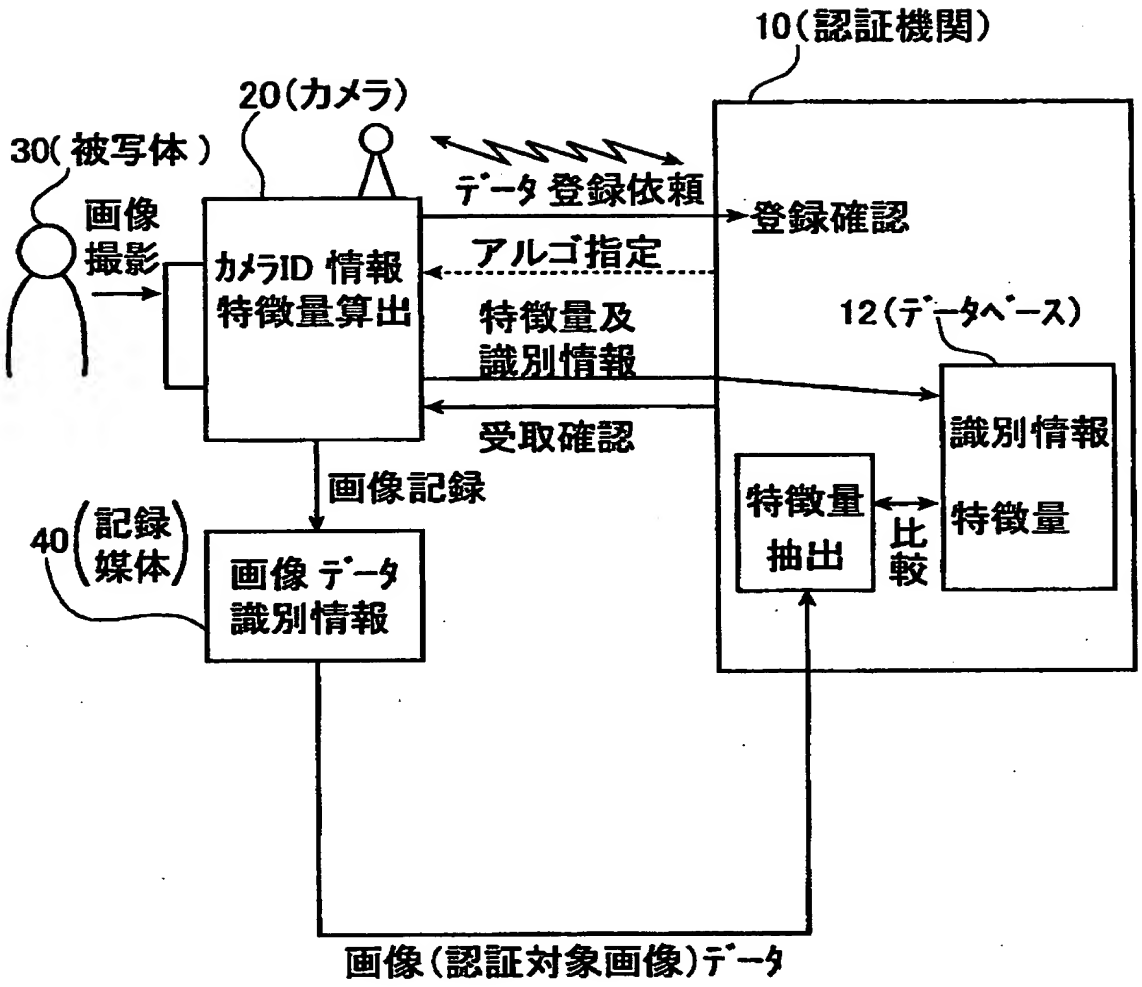
２０、６０　カメラ

３０、７０　被写体

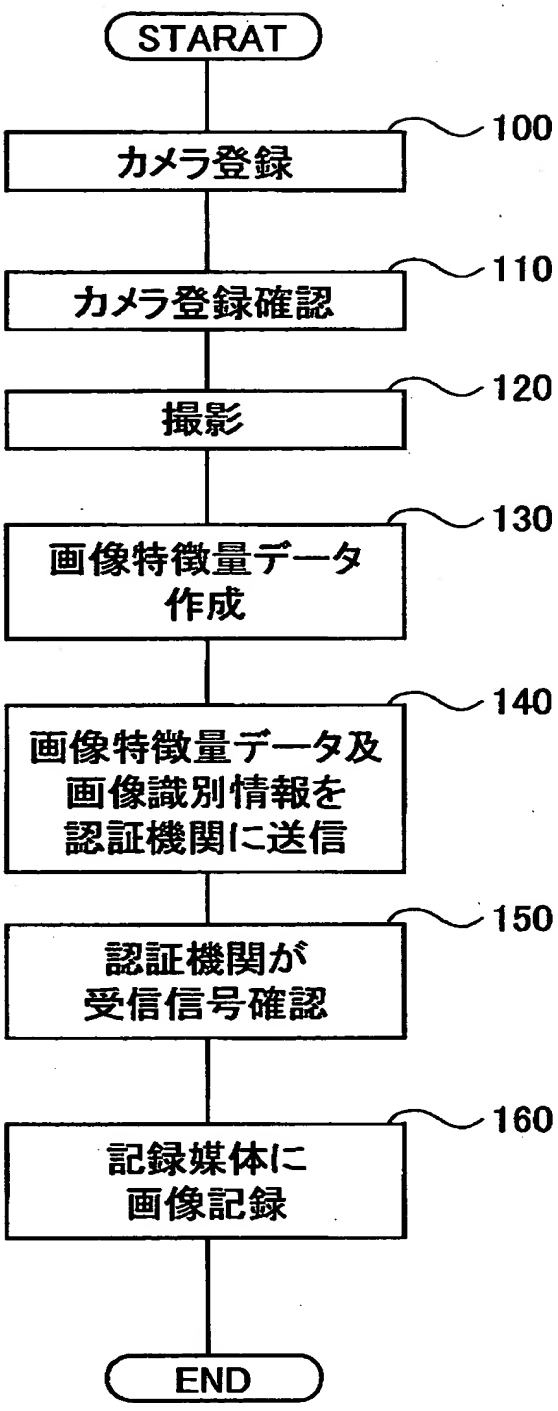
４０、８０　記録媒体

【書類名】　　図面

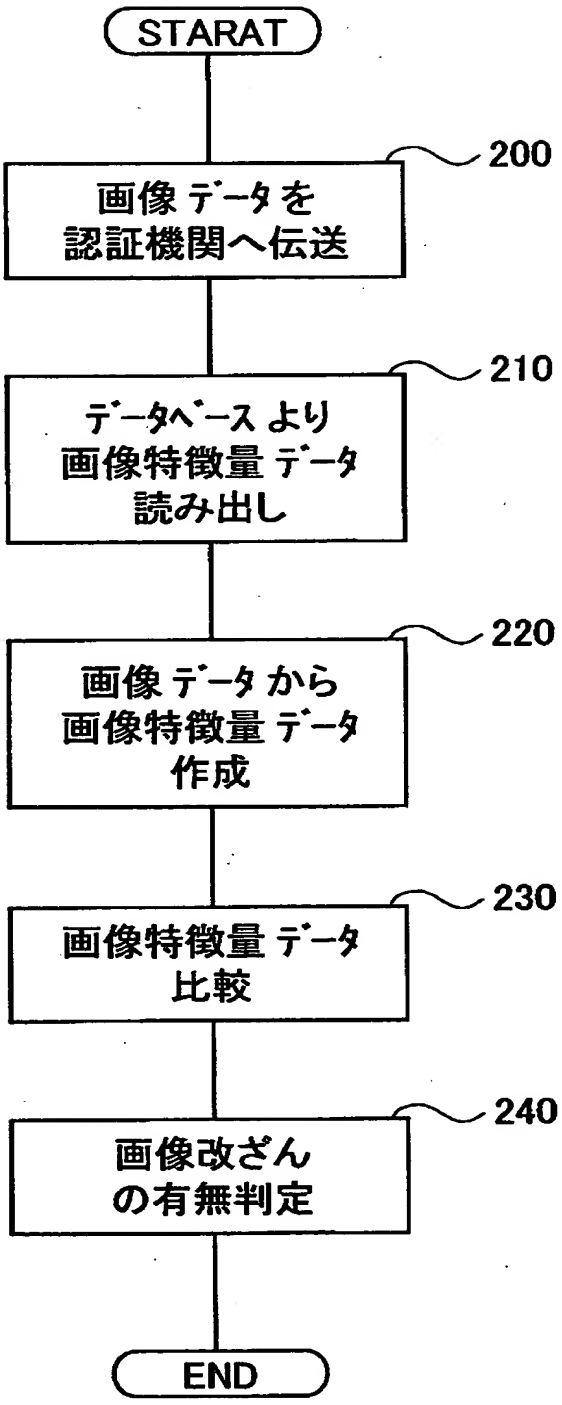
【図１】


10(認証機関)
20(カメラ)
30(被写体)
画像
撮影
カメラID 情報
特徴量算出
データ登録依頼
登録確認
アルゴ指定
特徴量及
識別情報
受取確認
12(データベース)
識別情報
特徴量
特徴量
抽出
比較
画像記録
40
記録
媒体
画像データ
識別情報
画像(認証対象画像)データ

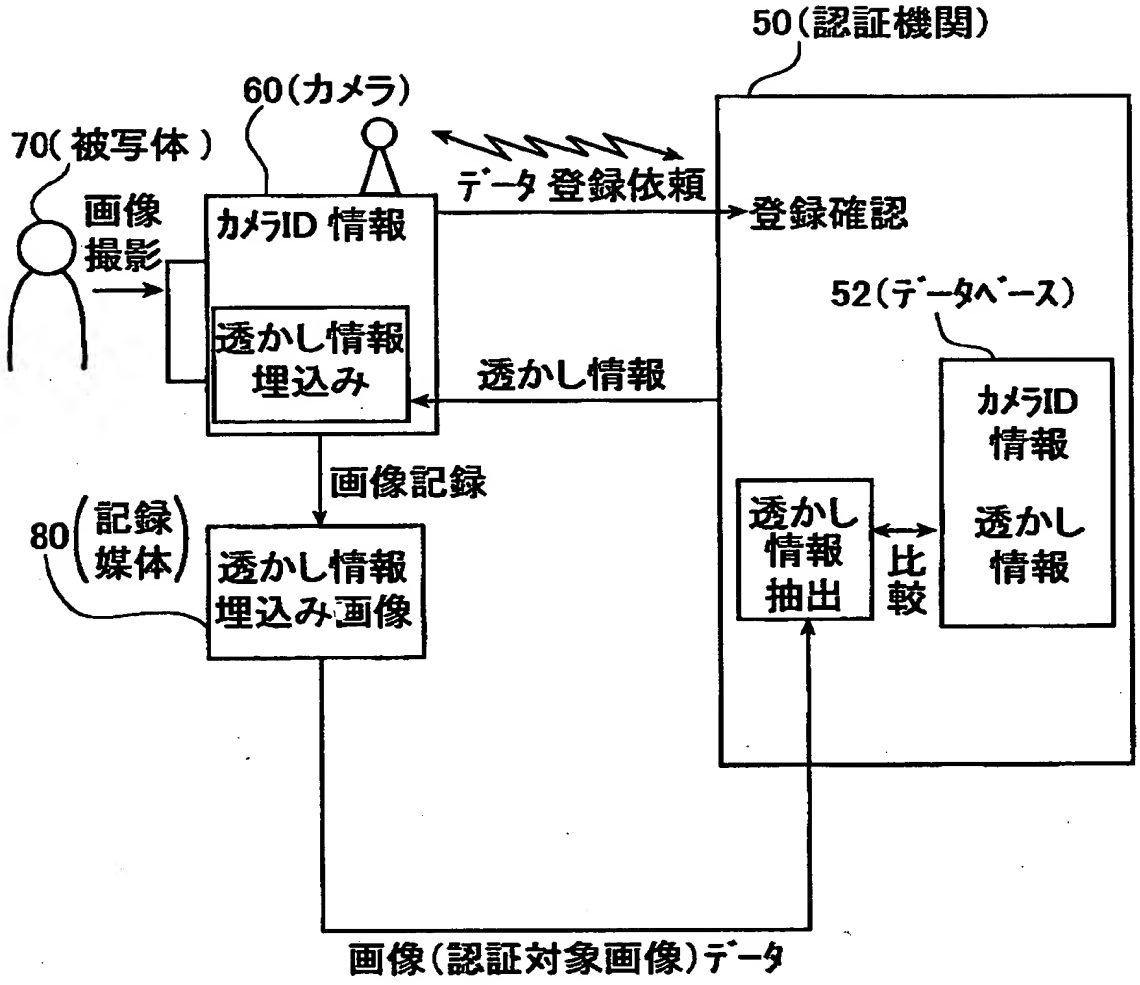
【図２】


STARAT
カメラ登録
100
カメラ登録確認
110
撮影
120
画像特徴量データ
作成
130
画像特徴量データ及
画像識別情報を
認証機関に送信
140
認証機関が
受信信号確認
150
記録媒体に
画像記録
160
END

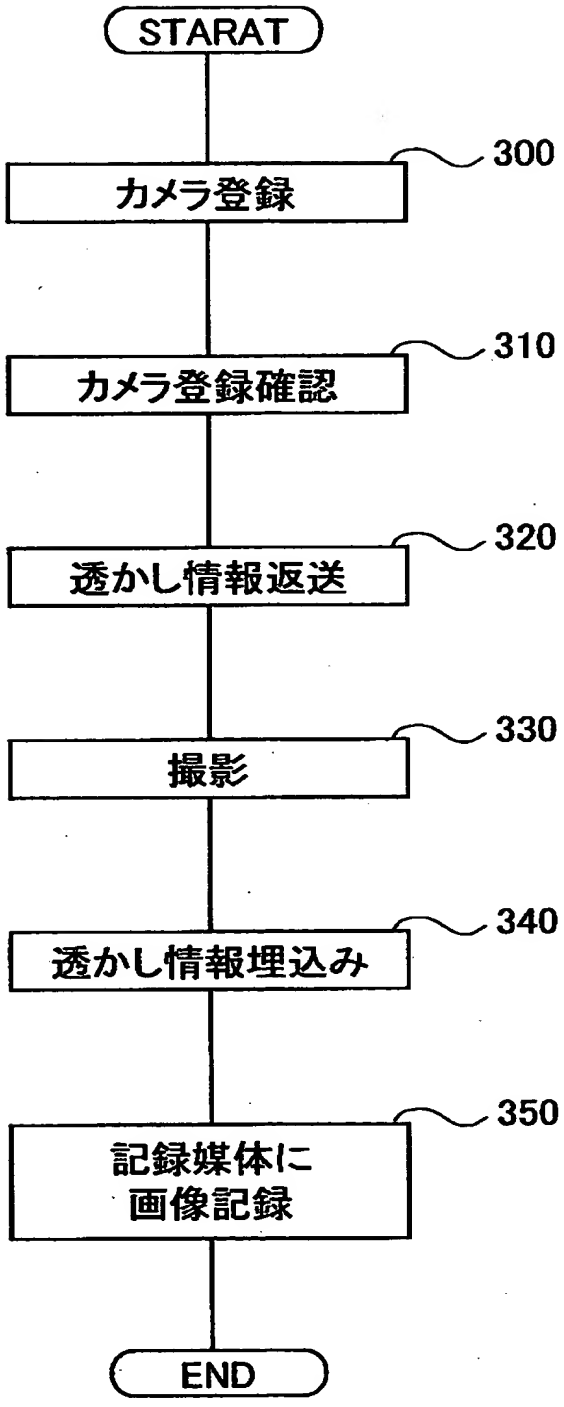
【図３】


STARAT
200
画像データを
認証機関へ伝送
210
データベースより
画像特徴量データ
読み出し
220
画像データから
画像特徴量データ
作成
230
画像特徴量データ
比較
240
画像改ざん
の有無判定
END

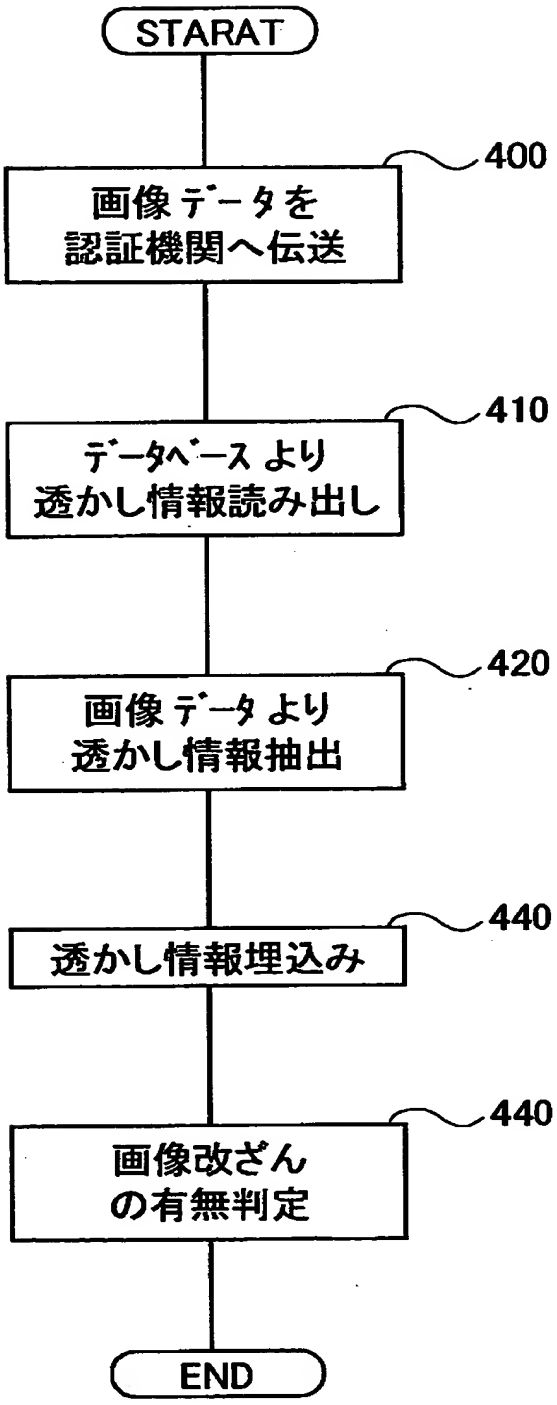
【図４】


50(認証機関)
60(カメラ)
70(被写体)
画像
撮影
カメラID 情報
データ登録依頼
登録確認
52(データベース)
透かし情報
埋込み
透かし情報
カメラID
情報
透かし
情報
画像記録
80
記録
媒体
透かし情報
埋込み画像
透かし
情報
抽出
比
較
画像(認証対象画像)データ

【図５】


STARAT
300
カメラ登録
310
カメラ登録確認
320
透かし情報返送
330
撮影
340
透かし情報埋込み
350
記録媒体に
画像記録
END

【図６】


STARAT
400
画像データを
認証機関へ伝送
410
データベースより
透かし情報読み出し
420
画像データより
透かし情報抽出
440
透かし情報埋込み
440
画像改ざん
の有無判定
END

【書類名】　　要約書

【要約】

【課題】特殊な機能を持たせた記録媒体を必要とせずに、画像の改竄がないことを認証する。

【解決手段】カメラにおいて、撮影画像から特定アルゴリズムにより画像特徴量を抽出し、カメラの撮影画像識別情報と前記画像特徴量を、撮影画像に改竄がないことを認証する認証機関のデータベースに記録し、前記認証機関において、認証することを請求された認証対象画像について、該認証対象画像から前記特定アルゴリズムにより画像特徴量を抽出し、該抽出された画像特徴量を前記データベースに記録された画像特徴量と比較し、該比較における両画像特徴量の一致度により、前記認証対象画像に撮影後の改竄がないことを判定することにより前記課題を解決する。

【選択図】図１

出願人履歴情報

識別番号　〔０００００５２０１〕

１．変更年月日　１９９０年　８月１４日
［変更理由］　新規登録
住　所　神奈川県南足柄市中沼２１０番地
氏　名　富士写真フイルム株式会社